RECEIVED
CENTRAL FAX CENTER
SEP 12 2007

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows, and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application claims indicated as cancelled.

1. (Currently Amended) A method comprising:

receiving a data frame, said data frame comprising a header and a data portion, the header comprising one or more of the group consisting of: a frame length, an encryption key, and an initial vector;

if one or more of the frame length, the encryption key, and the initial vector in the header indicates transmitting, configuring a transmitter to encrypt the data frame; and

if one or more of the frame length, the encryption key, and the initial vector in the header indicates receiving, configuring a receiver to decrypt the data frame.

2. (Original) The method of claim 1, further comprising authenticating the header of the data frame.

3. (Cancelled)

4. (Previously Presented) The method of claim 1 wherein configuring the receiver comprises:

configuring the receiver to authenticate and decrypt a data portion and a message integrity code portion of the data frame.

5. (Original) The method of claim 4 comprising:

decrypting the data portion and the message integrity code portion of the data frame to provide a decrypted data portion and a decrypted message

integrity code portion, respectively;

calculating the message integrity code of the data frame from the decrypted data portion; and

comparing the calculated message integrity code to the decrypted message integrity code portion.

6. (Previously Presented) The method of claim 1, wherein configuring the transmitter comprises:

configuring the transmitter to authenticate and to encrypt the data portion and a message integrity code based on information included in the header of said data frame.

7. (Original) The method of claim 6, further comprising:

dividing the data portion into two or more blocks of a predetermined block size; and

padding a last block of the data portion with one or more zeros to match the predetermined block size.

8. (Original) the method of claim 1 further comprising:

generating an encryption vector to be used to encrypt and decrypt the data frame.

9. (Original) The method of claim 1, further comprising:

generating an authentication vector to be used to authenticate the data frame.

10. (Original) The method of claim 8, further comprising:

decrypting one or more encrypted portions of the data frame by performing an exclusive OR operation between the one or more encrypted portions of the data frame and the encryption vector.

11. (Original) The method of claim 8, further comprising:

encrypting one or more portions of the data frame by applying an exclusive OR operation between the one or more portions of the data frame and the encryption vector.

12. (Currently Amended) An apparatus comprising:

a transmitter to encrypt a data frame;

a receiver to decrypt the data frame; and

a configuration unit to configure the transmitter and the receiver based on information included in the data frame;

wherein the information included in the data frame comprises one or more of the group consisting of: a frame length, an encryption key, and an initial vector.

13. (Original) The apparatus of claim 12, comprising:

a security unit to provide an encryption vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.

14. (Original) The apparatus of claim 12, comprising:

a security unit to provide an authentication vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.

15. (Original) The apparatus of claim 13, wherein the receiver includes a decryption unit to provide a decrypted data frame by applying the encryption vector to an encrypted data frame.

16. (Original) The apparatus of claim 13, wherein the transmitter includes an encryption unit to receive an authenticated data frame and the encryption vector to provide an encrypted data frame.

17. (Original) The apparatus of claim 13, wherein the security unit comprises:

an advance encryption standard engine to generate the encryption vector and an authentication vector.

18. (Original) The apparatus of claim 13, wherein the security unit comprises:

a message integrity code generator to generate a message integrity code of the encrypted data frame and to calculate a message integrity code of a decrypted data message.

19. (Original) The apparatus of claim 18, wherein the security unit comprises.

a comparator to compare between the calculated message integrity code and a decrypted message integrity code.

20. (Cancelled)

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Cancelled)

25. (Cancelled)

26. (Currently Amended) A wireless communication system comprising:

two or more stations wherein at least one station of the two or more stations includes:

a transmitter to encrypt a data frame;

a receiver to decrypt the data frame; and

a configuration unit to configure the transmitter and the receiver based on information included in the data frame;

wherein the information included in the data frame comprises one or more of the group consisting of: a frame length, an encryption key, and an initial vector.

27. (Original) The apparatus of claim 26, comprising:

a security unit to provide an encryption vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.

28. (Original) The apparatus of claim 26, comprising:

a security unit to provide an authentication vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.

29. (Original) The apparatus of claim 27, wherein the receiver comprises a decryption unit to provide a decrypted data frame by applying the encryption vector to an encrypted data frame.

30. (Original) The apparatus of claim 27, wherein the transmitter comprises an encryption unit to receive an authenticated data frame and the encryption vector to provide an encrypted data frame.

31. (Original) The apparatus of claim 27, wherein the security unit comprises:

an advance encryption standard engine to generate the encryption vector and an authentication vector.

32. (Currently Amended) An article comprising: a storage medium, having stored thereon instructions, that when executed, result in:

receiving a data frame, said data frame comprising a header and a data portion, the header comprising one or more of the group consisting of: a frame

length, an encryption key, and an initial vector;

if one or more of the frame length, the encryption key, and the initial vector in the header indicates transmitting, configuring a transmitter to encrypt the data frame; and

if one or more of the frame length, the encryption key, and the initial vector in the header indicates receiving, configuring a receiver to decrypt the data frame.

33. (Previously Presented) The article of claim 32, wherein the instructions when executed, result in:

configuring the receiver to authenticate and decrypt the data portion and a message integrity code portion of the data frame.

34. (Previously Presented) The article of claim 32, wherein the instructions when executed, result in:

generating an encryption vector to be used to encrypt and decrypt the data frame based on information included in the header of the data frame.

35. (Previously Presented) The article of claim 32, wherein the instructions when executed, result in:

generating an authentication vector to be used to authenticate the data frame.

36. (Previously Presented) The article of claim 32, wherein the instructions when executed, result in:

decrypting one or more encrypted portions of the data frame by performing an exclusive OR operation between the one or more encrypted portions of the data frame and the encryption vector.